RSAC 2025 Conference

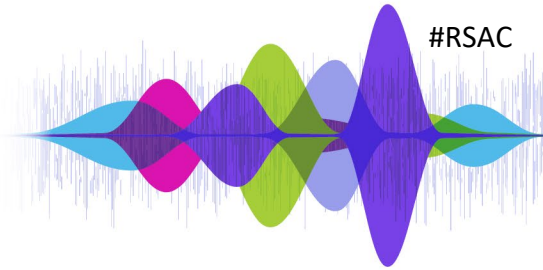
Many Voices.
One Community.

SESSION ID: FND-M01

Practical Strategies for Security Architecture in a Changing World

Abhilasha Bhargav-Spantzel

Partner Security Architect
Microsoft
linkedin.com/in/bhargav/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Agenda

- The Architectural Mindset
- Security & Compliance by Design
- Core Pillars of Security Architecture
- Threat Modeling & Resilience Testing
- Holistic System Thinking
- Open Source, Standards & Emerging Trends
- Call to Action

The Architectural Mindset – Form Follows Function

Vitruvius emphasized the triad of Function, Strength, and Beauty in architecture around 30 BCE, shaping early architectural mindset.

In the 1920-30s, the Bauhaus school promoted ‘Form Follows Function’ - Louis Sullivan (1852). Le Corbusier, Swiss-French architect, promoted standardization, defense in depth and “machine for living”.

...

Today, these foundational ideals converge to guide modern software and security architectures, delivering robust, user-centric, and elegantly designed systems.

Security & Compliance by Design

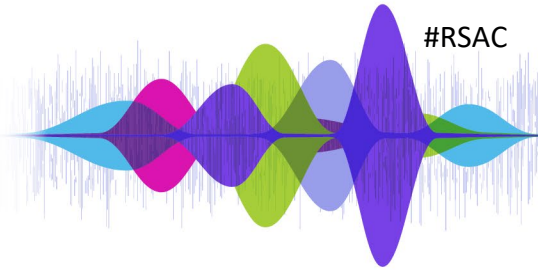
- Policy as Code
- Continuous Auditing & Monitoring
- Code Scanning (AI Analysis of Source Code)
- DevSecOps – Training + Tooling

```
package example.allow_access

default allow = false

allow {
    input.user == "admin"
    input.action == "write"
}
```

GDPR, | CCPA | NIST | ISO 27001

Phase	Security Integration
Requirements & Design	Threat modeling, secure architecture reviews, compliance checks.
Development	Secure coding practices, static code analysis (SAST), dependency scanning.
Build & CI/CD	Automated security tests, dynamic application security testing (DAST).
Testing & Deployment	Runtime security scans, container security checks.
Operations & Monitoring	Continuous security monitoring, intrusion detection, vulnerability management.

Security & Compliance by Design



Phase	Security Integration
Requirements & Design	Threat modeling, secure architecture reviews, compliance checks.
Development	Secure coding practices, static code analysis (SAST), dependency scanning.
Build & CI/CD	Automated security tests, dynamic application security testing (DAST).
Testing & Deployment	Runtime security scans, container security checks.
Operations & Monitoring	Continuous security monitoring, intrusion detection, vulnerability management.

Core Security Pillars

Identity Protection

- Ensuring secure and verified access control to prevent unauthorized access and protect sensitive information.

Data Protection

- Protecting sensitive and critical information from unauthorized access, leaks, and breaches to maintain data integrity.

Threat Intelligence

- Gathering and analyzing threat information to stay ahead of potential security risks and enhance defense strategies.

Resilience and Patching

- Maintaining system robustness and promptly addressing vulnerabilities through regular updates, incident response and patch management.

Core Security Pillars - Identity

Multi-Factor Adaptive Authentication

- Password-less auth: biometrics, etc.
- Hardware-based auth: FIDO2, smart cards, TPM

Inclusive Authentication

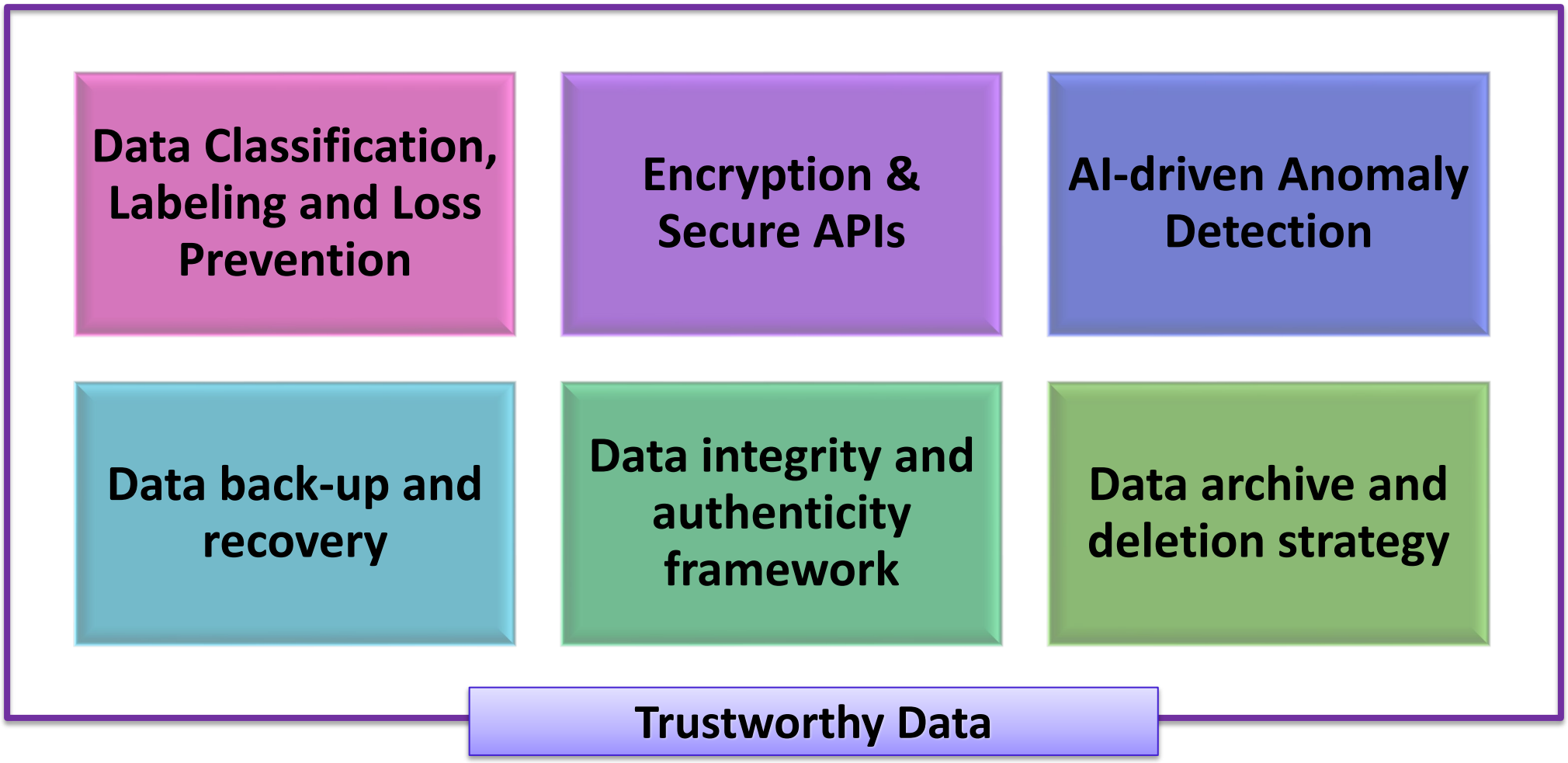
Zero Trust & Least Privilege

Continuous Authentication

Identity governance

PIM account handling

Core Security Pillars - Data


Data Classification, Labeling and Loss Prevention
Encryption & Secure APIs
AI-driven Anomaly Detection
Data back-up and recovery
Data integrity and authenticity framework
Data archive and deletion strategy
Trustworthy Data

Core Security Pillars - Threat Intelligence

- AI-Generated Threats
- MITRE ATLAS & OWASP LLM
- AI-Driven Threat Hunting
- Insider Threats
- Nation State Attacks
- ISAC/OSINT

Core Security Pillars - Resilience & Patching

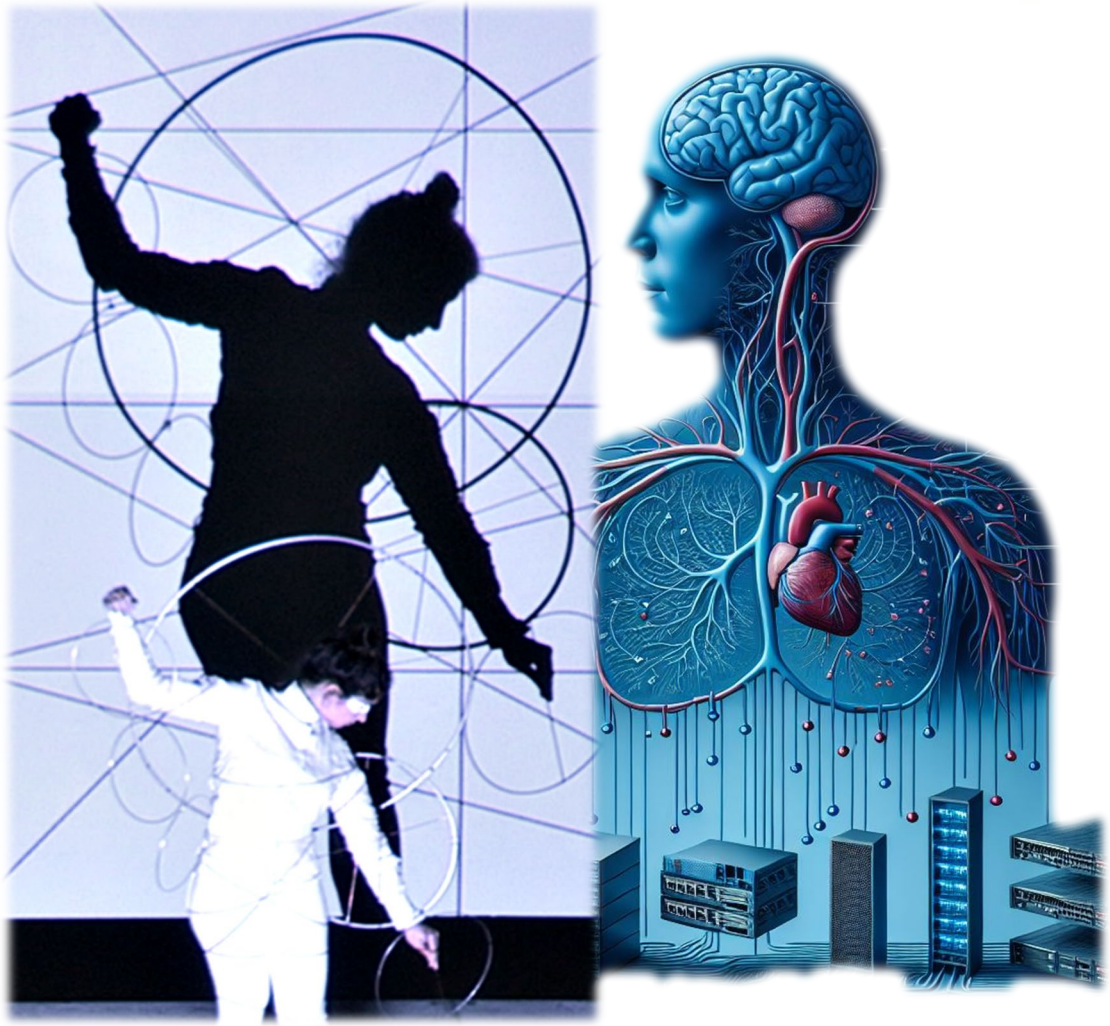
- Patch Velocity
- Supply Chain Security
- AI-powered Anomaly Detection
- Automated patch management
- User education/training

Effective and Efficient Threat Modeling

1	Know your product	• Functionality, Security & Privacy
2	Know your assets	• Scope your critical assets
3	Know your adversaries and risks	• Sophisticated adversaries • Insider Risk
4	Build Mitigations - Security by Design	• Built-in security features and mitigations

Holistic System Thinking

- Security as a System
- Holistic Diagnosis
- Supply chain and dependency view
- Feedback loops and early warning
- Resilience and redundancy



Open Source, Standards & Emerging Trends

Open Source Security & Software Supply Chain

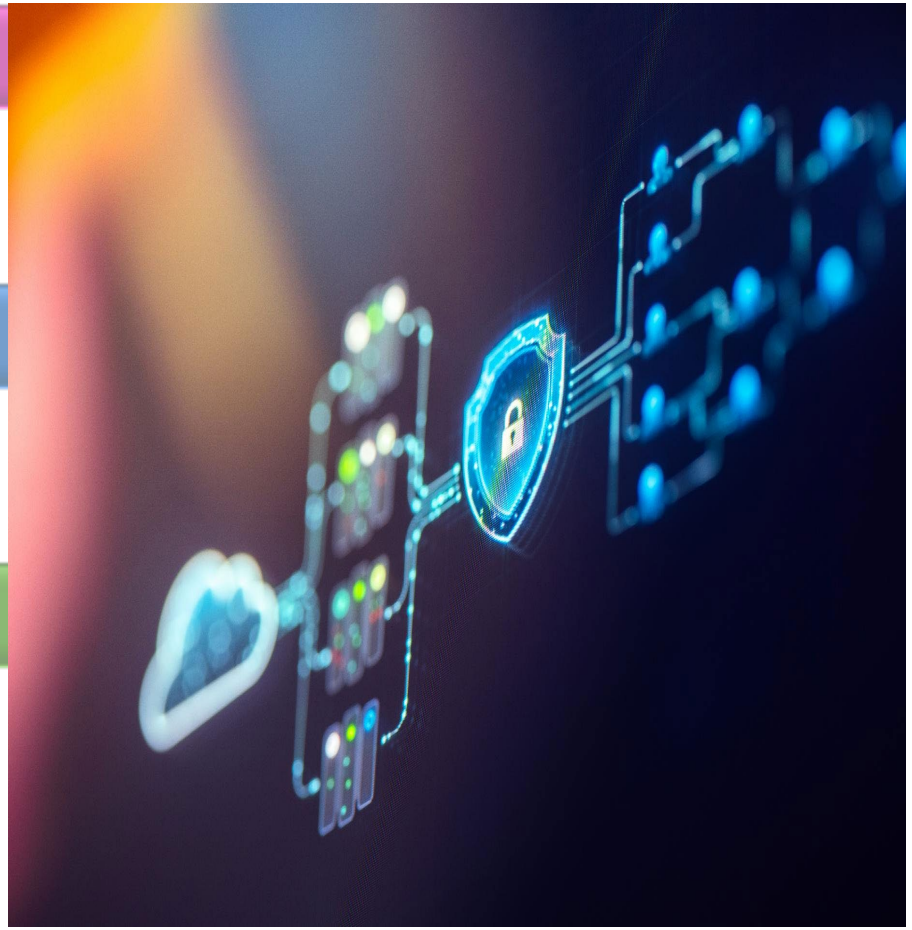
- Software Bill of Materials (SBOM) (e.g., SPDX, CycloneDX)
- Provenance & Trust (e.g., Sigstore for verifying provenance)
- Dependency Scanning and continuous Software Composition Analysis (SCA)

Security Standards & Frameworks

- ISO 27001, NIST SSDF (Secure Software Development Framework), OWASP
- Regulatory compliance trends (e.g., GDPR, CCPA for data privacy)
- Emerging or newly updated frameworks for cloud-native and AI security

Emerging Threats & Techniques

- Model Poisoning & Data Poisoning (adversarial attacks on ML pipelines)
- Pickling Attacks in Python (insecure deserialization)
- Supply-Chain Attacks (e.g., SolarWinds, dependency confusion)
- Potential vulnerabilities in Large Language Models (LLM-based systems)



Summary
Architecting for the Future

Embed Security in Design

Iterative Threat Modeling

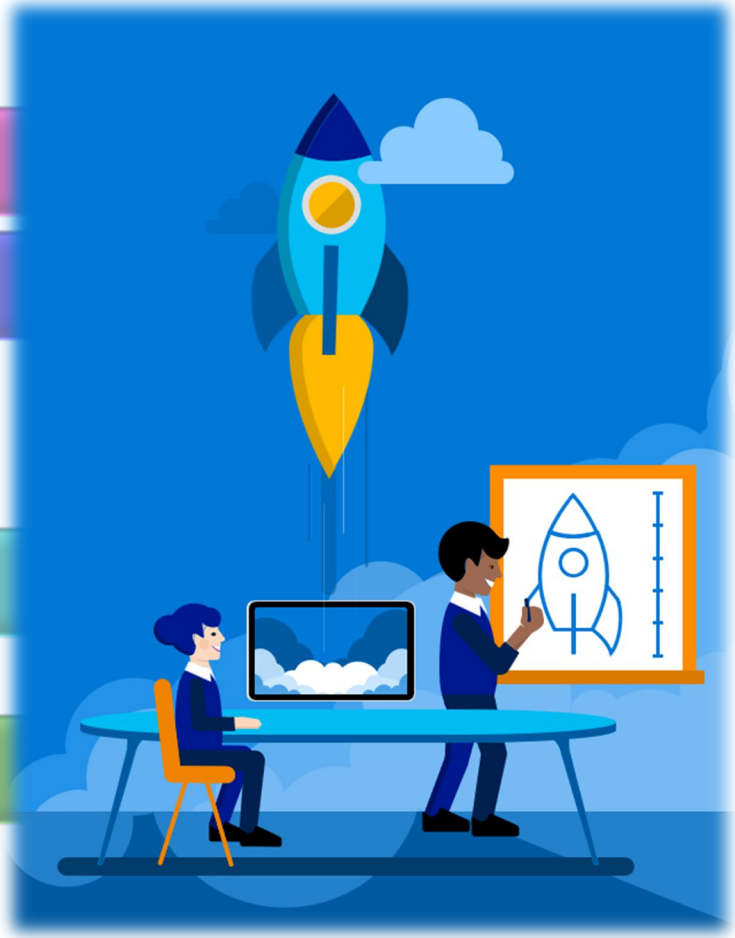
- Know your assets
- Inventory critical systems, data, applications, business processes
- Adapt to Emerging Threats

Automate Compliance & Governance

- Culture, user behavior and processes

Socio-Technical Integration

- Safety and Responsibility



Apply What You Have Learned Today

Next week

Critical Infrastructure Inventory – Know your assets

Know about Biz Requirements, Compliance and Governance

In first 3 months

Embed Security in Design: Start Green.

Iterative Threat Modeling: Stay Green

Culture, User Behavior and Awareness

- Training Documentation and reduced Human Error

Within six months

Adapt to Emerging Threats

Trust but Verify - Conduct regular security reviews, pen testing, and red team exercises

Ensure a feedback loop to help security by design and security by default

References & Further Reading

Security Frameworks

NIST Cybersecurity Framework, MITRE ATT&CK, and CIS Controls provide comprehensive guidelines for enhancing security measures.

Data Regulation with GDPR, CCPA, Privacy and Data Protection

Zero Trust & Cloud Security

Zero Trust Architecture (NIST 800-207) and Cloud Security Handbook offer strategies to secure cloud environments and infrastructure.

CSA STAR Program, SBOM & Software Supply Chain (SPDX, CycloneDX, Sigstore)

AI and Advanced Security Resources

MITRE ATLAS and OWASP LLM Top 10 are essential resources for understanding and implementing AI security measures

NIST Post Quantum Crypto (PQC) Project and Quantum-Resistant Cryptography

RSAC 2025 Conference

Acknowledgement

Big Thank You to fellow architects Ed Moyle and Jordan Hull for their excellent feedback and support for this presentation! 😊

Many Voices.
One Community.

RSAC™ 2025 Conference

Thank you!

Many Voices.
One Community.